

2007 Security Incites

What are the Security Incites?

Annually, Security Incite publishes a list of the key “trends” in the security business for the next year. Called “Security Incites” and written from the perspective of the end user (or security consumer), Incites provide direction on what to expect, assisting the decision making process as budgets and technology adoption plans are finalized for the upcoming year. Each Incite provides a clear position and distills the impact on buying dynamics and architectural constructs. Incites also set the stage for Security Incite’s upcoming research agenda.

2007 Security Incites

1. Get with the Program

As security professionals continue to struggle with the number of threats and contradictory goals (protect information, but assist business), they increasingly turn to structured security programs (ISO 27001, COBIT, Pragmatic CSO) to assist in getting things done and communicating progress. Security management tools (predominately SIEM) continue to leave customers wanting for value and assistance in automating programmatic operations.

2. CSO Next

A new breed of CSO emerges in 2007, focused on running security as a business. High visibility, setting milestones, communicating progress, prioritizing fiercely, outsourcing strategically, managing vendors aggressively, and embracing advisors and coaches are the hallmarks of “CSO Next.” This Pragmatic CSO needs to look more like an MBA-type than a code jockey, which creates many challenges for the current generation of technically-oriented CSO.

3. Perimeter (R)Evolution

The consolidated perimeter platform continues to subsume additional security and networking functions, making top flight content security and application acceleration the next frontier – further squeezing pure-play security players. This accelerates consolidation in the sector, keeping perimeter architectures in flux. Customers increasingly embrace integrated solutions from larger players putting a “best of breed” mindset on life support and proving that “big is the new small.” The first open source perimeter platforms also hit in 2007, providing a legitimate alternative for technically savvy, mid-sized businesses.

4. Trust No One

The “insider threat” continues to garner tremendous hype, but leaves customers struggling to figure out muddled offerings and providing disappointing results for early adopters. The NAC (network access control) bubble pops rather visibly in a maelstrom of confusion, forcing users to focus on solving specific problems (like visitor and contractor access) and implementing monitoring processes which result in checks and balances at all levels of the organization.

5. You (Mal)ware It Well

The most significant innovations in 2007 come from the bad guys continuing to find new ways to compromise desktops and install rootkits/Trojans and other bad stuff, resulting in the first million bot network. Big AV responds with more integrated suites, but remains under siege from new entrants looking to milk the AV cash cow. For users, the best defense turns out to be a good offense as Pragmatic CSOs spend significant time and effort training users and pushing ISPs to address the damage of rampant bot activity.

6. Patching the Leaks

More high profile privacy train wrecks force many customers to just buy something to address the information leakage problem. Laptop encryption turns out to be far from a panacea, while multi-protocol leak prevention gateways remain in high demand. Users demand integration at both ends (client and perimeter), foreshadowing more consolidation. Users finally figure out data protection is more of a process issue, forcing Pragmatic CSOs to ask tough questions of senior IT managers on how data is handled and who has access to it.

7. The Information Strikes Back

2007 finally brings acknowledgement that data/information security is different than protecting the network and servers. Yet, there is a major skills shortage in folks that understand how to protect applications and databases, resulting in accelerating interest in application and database security product offerings. But history will repeat itself, as a “fool with a tool” is still a fool, which doesn’t help customers solve any problems.

8. Identity Everywhere

Identity becomes the most overused term in 2007, as NAC vendors, systems management vendors, Big Security, and everyone else “identity-enable” their offerings more as a marketing initiative than to add value. Pragmatic CSOs focus on solving problems, embracing non-disruptive mutual authentication and integrating directory stores with network equipment to streamline management

and problem isolation. The first inklings of an interoperable “identity network” emerge, making cheap multi-use tokens more compelling to a broader market.

9. Help Wanted: Fortune Teller

CSOs need to increasingly flex their psychic abilities as exponentially increasing attack surfaces mean new controls must be targeted to protect the most likely targets, which are identified by discerning the true value of corporate business systems and increasingly sophisticated (and productized) security research. Network behavior analysis allows organizations to “react faster” by understanding network traffic dynamics, but integration with remediation solutions lag, forcing customers to continue to do the heavy lifting themselves.

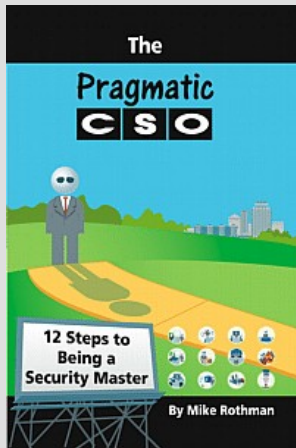
10. Time to get PC(I)

PCI is the new SarbOx as unsophisticated CSOs continue to try to “buy” compliance. The lack of regulatory enforcement and increasing scrutiny by bean counters finally kill compliance’s golden goose and force CSOs to justify more security spending on something other than compliance. Pragmatic CSOs understand that a strong security program addresses compliance requirements, so they focus on warming relations with auditors and communicating their results in business terms to the business people that matter.

About Security Incite

Security Incite is an industry analyst firm specializing in the information security market. Our mission is straightforward: Help subscribers protect their information assets more effectively by making better decisions. Security Incite was founded to address a real need to provide objective, relevant and inciteful security research by focusing on what's right, as opposed to what pays well. Focusing on bold, thought-provoking and irreverent analysis, Security Incite helps organizations make better decisions. Our tagline is "No Bias. No Bull. Real Incite," which does a good job of explaining our philosophy and our focus.

Security Incite publishes *The Daily Incite*, a unique, refreshing, no holds barred newsletter about the information security business. And you never know who is going to be on the receiving end of one of President Mike Rothman's famous rants. As a bonus, subscribers also receive Security Incite's BUYING SECURITY PRODUCTS ebook. To subscribe, send email to dailyincite@securityincite.net or visit <http://securityincite.com/dailyincite>.



The attacks have changed. Why are you doing the same old security stuff?

Chief Security Officers have been locked in a LOSING BATTLE with the bad guys. Senior management is losing faith and scrutinizing security activities. We need a new way to "do" security - a program that gets you to focus on protecting what's important, to stop chasing the attack de jour, and to keep the auditors in check.

This new way is **The Pragmatic CSO.**

Buy the new Book from Security Incite's Mike Rothman and learn a 12-step program to become a better CSO. It's available now at www.pragmaticcso.com.

I strongly recommend buying and reading The Pragmatic CSO. All CSOs should also have a copy, period.
- Richard Bejtlich

This is the first time I have read a book about security that not only made sense, but actually gave some decent advice on how to do something about it.
- Mike Murray (www.episteme.ca)

Mike Rothman's The Pragmatic CSO presents a fresh, human approach to the intimidating world of managing enterprise security.
- Ken Camp

I think the Pragmatic CSO will go down as a milestone in the security management arena.
- Alan Shimel